

Notice of Allowability

Application No.

09/821,565

Applicant(s)

ISHIKAWA, MARK M.

Examiner

Tongoc Tran

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 5/23/2006 and interviews held on 6/20/06 and 6/22/06.
2. ☒ The allowed claim(s) is/are 40-53, 56-58, 70-78 and ⁶⁰⁻⁶⁸~~66-68~~.
3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some* c) ☐ None of the:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
- (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
- 1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
- (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date _____
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____

Jacques H. Louis Jacques
JACQUES H. LOUIS JACQUES
PRIMARY EXAMINER

DETAILED ACTION

1 An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Davin M. Stockwell on June 22, 2006.

Claims:

Claim 40:

- On line 13, "and" has been deleted.
- On line 20, "*providing* the network address of the second network device to the first network device," has been replaced with - - *broadcasting* the network address of the second network device to the first network device, - -
- At the end of the claim, insert "; and a firewall system that identifies suspect information packets received from the first network device, said switching system directing the information packets to the second network device via said firewall system, wherein said traffic analysis system determines whether the suspect information packets are problematic and, if said traffic analysis system determines that the suspect information packets are problematic,

inhibits said switching system from broadcasting the network address of the second network device to the first network device”.

Claims 54 and 55 have been canceled.

Claim 56:

- On line 6, “and” has been deleted.
- On lines 12-13, “*providing* the network address of the second network device to the first network device” has been replaced with - - *broadcasting* the network address of the second network device to the first network device - -
- At the end of the claim, insert “; and said activity monitoring system includes: a route arbitration system that monitors the information packets received by said switching system, said route arbitration system determining whether the information packets comprise abnormal network activity in accordance with a first information packets comprise abnormal network activity, identifying the information packets are being abnormal information packets; and a traffic analysis system that monitors the abnormal information packets identified by said route arbitration system, said analysis system determining whether the abnormal information packets comprises the problematic information packets in accordance with a second predetermined criteria and, if said traffic analysis system determines that the abnormal information packets comprise the problematic information packets, inhibiting said switching system from providing

the network information packets, inhibiting said switching system from broadcasting the network address of the second network device to the first network device”

Claim 59 has been canceled.

Claim 60:

- On line 12, “and” has been deleted.
- On lines 10-20, “*providing* the network address of said protected network device to the external network device” has been replaced with - - *broadcasting* the network address of said protected network device to the external network device - -
- At the end of the claim, insert “; and a firewall system that identifies suspect information packets received from the external network device, said switching system directing the information packets to the protected network device via said firewall system, said traffic analysis system determining whether the suspect information packets are problematic and, if said traffic analysis system determines that the suspect information packets are problematic, inhibiting said switching system from broadcasting the network address of the protected network device to the external network device”

Claim 69 has been canceled.

Claim 71:

- On line 14, "and" has been deleted.
- On lines 18-19, "*providing* the network address of said second network device to the first network device" has been replaced with - - *broadcasting* the network address of said second network device to the first network device - -
- At the end of the claim, insert "; and a firewall system that identifies suspect information packets received from the external network device, said switching system directing the information packets to the protected network device via said firewall system, said monitoring system determining whether the suspect information packets are problematic and, if said monitoring system determines that the suspect information packets are problematic, inhibiting said switching system from broadcasting the network address of the protected network device to the external network device".

Claim 77:

- On line 9, "and" has been deleted.
- On lines 13-14, "*providing* the network address of said second device to the first network device" has been replaced with - - *broadcasting* the network address of said second device to the first network device - -.
- At the end of the claim, insert "; and a firewall system that identifies suspect information packets received from the external network device, said switching

System directing the information packets to the protected network device via said firewall system, said monitoring system determining whether the suspect information packets are problematic and if said monitoring system determines that the suspect information packets are problematic, inhibiting said switching system from broadcasting the network address of the protected network device to the external network device”.

Claims 79 and 80 have been canceled.

Allowable Subject Matter

2. The following is an examiner's statement of reasons for allowance:

The claimed invention is directed to detection of fraudulent requests and eradicates the request from attacking the target network resource. The detection system and method monitor the incoming network activities arriving at the network devices such as routers and firewalls and determining whether abnormal activities or traffic patterns are emerging the devices. If a determination is made that the patterns exist, the monitoring system responds by blocking the activity or redirecting the traffic.

The closest prior art, Shanklin et al., teach an intrusion detection system with load balancing for high-speed networks. The system detects unauthorized signatures to or from local network and connected at an internetworking device such as a router or a switch. Shanklin et al. teach after detection of unauthorized activities exist, the system response by taking appropriate actions such as disconnect the network communication.

Art Unit: 2134

Shanklin et al do not disclose the detail of specific appropriate functionality the network would take in response to the detection except terminating the connection. Applicant claims the unique features of a router arbiter and a firewall for redirecting the abnormal traffic to the traffic analyzer to further determine whether the abnormal information packets are problematic in accordance to different set of criteria, if problematic information packets is determined to exist, inhibiting the switching system from broadcasting the network address to the offending device. The network device as claimed is interpreted in light of the Specification to be a router or a firewall. The art of record does not singularly or in combination anticipate or render the claimed limitation obvious.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

3 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tongoc Tran whose telephone number is (571) 272-3843. The examiner can normally be reached on 8:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jacques Louis-Jacques can be reached on (571) 272-6962. The fax phone

Art Unit: 2134

number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

TT

Jacques H. Louis Jacques
JACQUES H. LOUIS JACQUES
PRIMARY EXAMINER